SEBASTIAN RIEGER

# MÜSSEN DATEN AUF ANTRAG STETS GELÖSCHT WERDEN?

## Grenzen der Betroffenenrechte im nDSG

**Das neue Datenschutzgesetz ist eine der wichtigsten Totalrevisionen der letzten Jahre. Mit dem neuen Gesetz stellen sich für Datenbearbeiter und Datenbearbeiterinnen zahlreiche Fragen. Insbesondere die Umsetzung der Pflichten stellen diese vor dem Hintergrund des strengen Sanktionsregimes vor neue Herausforderungen. Eine dieser Herausforderungen ist der Umgang mit Löschungsanträgen.**

### 1. EINLEITUNG

Am 25. September 2020 wurde das neue Datenschutzgesetz (nDSG) nach langem Hin und Her beschlossen. Die Totalrevision des aus dem Jahr 1992 datierenden Datenschutzgesetzes (DSG) war im Hinblick auf die technologische Entwicklung der letzten 30 Jahre, der rechtlichen Entwicklung in der EU und dem Inkrafttreten der DSGVO [1] angezeigt.

Der Datenschutz dient der Verwirklichung verfassungsmässiger Rechte. Damit die betroffenen Personen – insbesondere im digitalen Raum – ihre Rechte effektiver wahrnehmen können, sieht das nDSG zahlreiche Pflichten für Datenbearbeiter und Datenbearbeiterinnen vor.

Nachfolgend wird eine Auswahl dieser Neuerungen beleuchtet. Im Anschluss daran erfolgt eine Fokussierung auf das Widerspruchs- und das damit einhergehende Lösungsrecht der betroffenen Person.

### 2. GRUNDSÄTZLICHE ZULÄSSIGKEIT DER DATENBEARBEITUNG NACH SCHWEIZER DATENSCHUTZRECHT

Nach geltendem Datenschutzrecht ist die Bearbeitung von Personendaten nur dann zulässig, wenn sie rechtmässig, nach Treu und Glauben und verhältnismässig erfolgt [2]. Des Weiteren dürfen Personendaten nur zu dem bei der Beschaffung angegeben Zweck bearbeitet werden. Dieser Zweck muss aus den Umständen ersichtlich oder gesetzlich vorgesehen sein. Die Datenbearbeitung muss dabei für die betroffene Person erkennbar sein [3]. Der oder die Verantwortliche hat auch sicherzustellen, dass die Daten korrekt sind, die er oder sie bearbeitet (Grundsatz der Richtigkeit der Daten) [4].

Das nDSG übernimmt diese *Grundsätze* so weit wie möglich [5]. Entsprechend dienen sie in Zukunft als Leitlinie für jede Datenbearbeitung [6].

Sofern die Grundsätze eingehalten werden, ist die Datenbearbeitung rechtmässig und damit zulässig. Dies ist ein wichtiger Ansatz des Schweizer Datenschutzrechts, der auch nach neuem Recht gelten wird [7]. Anders sieht es in der EU aus. Dort ist die Verarbeitung personenbezogener Daten grundsätzlich verboten und nur im Einzelfall erlaubt, sofern einer der vorgesehenen Erlaubnistatbestände [8] erfüllt ist [9].

Neben den gleichbleibenden Grundprinzipien sieht das nDSG wesentliche Neuerungen vor. Insbesondere wird der Pflichtenkatalog erheblich erweitert [10] und das Sanktionssystem verschärft [11].

### 3. WESENTLICHE NEUERUNGEN: EINE AUSWAHL

Das nDSG sieht umfassendere Dokumentations- und Meldepflichten vor. Diese dienen als flankierende Massnahmen zu den eigentlichen Schutzpflichten.

Art. 12 nDSG sieht vor, dass jede verantwortliche Person und jeder Auftragsbearbeiter [12] ein *Verzeichnis ihrer/seiner Bearbeitungstätigkeit* führen muss. Dies wurde aus der DSGVO übernommen (Art. 30 DSGVO). Das Gesetz definiert den Mindestinhalt des Verzeichnisses. Eine Formvorschrift schreibt das nDSG nicht vor, dafür aber eine Ausnahme für KMU [13].

Des Weiteren sieht das nDSG vor, dass der oder die Verantwortliche vor einer allfälligen Bearbeitung vorgängig eine *Datenschutz-Folgenabschätzung* (DSFA) vornimmt, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Die DSFA dient also der Risikobewertung. Sie enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken sowie die Massnahmen [14]. Sie dient einerseits der Validierung von Risiken für den Datenschutz und ist entsprechend auch für ein Internes Kontrollsystem (IKS) nutzbar. Andererseits kann die korrekt vorgenommene datenschutzrechtliche Selbstbeurteilung auch aus Compliance-Sicht nützlich sein.

SEBASTIAN RIEGER, MLAW, ADVOKAT, DUFOUR ADVOKATUR, LEITER ABTEILUNG RECHT UND STEUERN PRO FONDS, DACHVERBAND GEMEINNÜTZIGER STIFTUNGEN DER SCHWEIZ

Neben der Pflicht, den oder die EDÖB [15] zu konsultieren, wenn die DSFA ein hohes Risiko prognostiziert, sieht das nDSG neu eine Pflicht zur Meldung von Datenschutzverletzungen *(Data Breach Notification)* an den oder die EDÖB vor [16]. Eine solche Meldepflicht gab es bis anhin nicht. Bisher galt die Meldepflicht lediglich in Bezug auf besonders schützenswerte Daten. Die Meldung hat so rasch als möglich zu erfolgen, in der EU innert 72 Stunden [17].

Neben den neuen bzw. erweiterten Dokumentations- und Meldepflichten sieht das nDSG auch erweiterte Pflichten für Datenbearbeiter und Datenbearbeiterinnen vor. Diese dienen primär dazu, dass die betroffene Person die ihr zustehenden Rechte auch effektiv wahrnehmen kann.

So sieht Art. 19 nDSG eine deutlich ausgebaute *Informationspflicht* vor [18]. Musste die betroffene Person bisher nur dann informiert werden, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile erstellt wurden [19], gilt dies neu für sämtliche Personendaten. Es besteht also eine proaktive Informationspflicht, unabhängig von der Datenkategorisierung. Natürlich sieht auch das nDSG diesbezügliche Einschränkungen vor (vgl. Art. 20 nDSG).

Wie die Information auszugestalten ist, sagt das nDSG nicht (keine Formvorschrift gemäss Art. 19 nDSG). In der Praxis wird die Information über die Datenbeschaffung allerdings meist in Form einer *Datenschutzerklärung* erfolgen. Nicht klar ist, ob eine mehrstufige Datenschutzerklärung zulässig ist. In der Lehre wird dies zwar bejaht [20]. Der erläuternde Bericht zum Vorentwurf der Verordnung zum nDSG (VDSG) hält jedoch fest, dass die Informationen auf der ersten Kommunikationsstufe zu erfolgen haben [21]. Nach Auffassung des Autors reicht der Verweis auf die Datenschutzerklärung aus, sofern der Zugriff auf die Informationen ohne Weiteres möglich und zumutbar ist. Auch in AGB oder anderen Unterlagen genügt i. d. R. der Hinweis auf die gleichzeitig verlinkte Datenschutzerklärung [22].

Wie bereits im geltenden DSG hat die betroffene Person *Anspruch auf Auskunft* (Art. 25 nDSG). Jede Person hat also das Recht, von der oder dem Verantwortlichen Auskunft darüber zu verlangen, ob Personendaten über sie bearbeitet werden. Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte effektiv geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Damit verwirklicht das Recht auf Auskunft einen Teil des verfassungsmässigen Rechts auf informationelle Selbstbestimmung [23].

## 4. DAS RECHT AUF LÖSCHUNG

Als wichtige Instrumente des informationellen Selbstbestimmungsrechts und damit des grundrechtlichen Datenschutzes dienen auch der Anspruch auf Berichtigung falscher Daten; der Anspruch auf Löschung ungeeigneter und nicht (mehr) benötigter Daten und der Anspruch auf Auskunft bzw. Einsicht [24]. Diese Instrumente finden sich auch im nDSG.

Die Datenbearbeitung ist in der Schweiz (anders als in der EU) unter Beachtung der Grundsätze zulässig. Das nDSG sieht entsprechend das *Opt-out-Prinzip* vor [25]. Soll keine Datenbearbeitung erfolgen, muss die betroffene Person dieser ganz oder teilweise widersprechen [26]. Ohne Widerspruch ist die Datenbearbeitung im gesetzlichen Rahmen zulässig. Als Kompensation dieses eher datenbearbeitungsfreundlichen Prinzips dürfen Personendaten nicht gegen den ausdrücklichen Willen der betroffenen Person bearbeitet werden [27].

Wie das geltende Recht sieht auch das nDSG ein *Widerspruchsrecht* vor. Eine betroffene Person kann sich gegen jeden Aspekt der Datenbearbeitung aussprechen, auch gegen die weitere Aufbewahrung ihrer Daten. Sie kann damit auch die Löschung ihrer Daten verlangen. Damit hat die Schweiz ebenfalls das in der DSGVO vorgesehene *Recht auf Vergessenwerden* in das nDSG implementiert [28].

Der implizite Löschungsanspruch gilt jedoch nicht absolut. Eine Datenbearbeitung, die trotz eines Löschungsbegehrens erfolgt, ist zwar rechtswidrig und stellt eine *Persönlichkeitsverletzung* dar (Art. 30 nDSG). Eine Persönlichkeitsverletzung ist aber nur dann widerrechtlich, wenn sie nicht durch ein überwiegendes privates oder öffentliches Interesse oder durch das Gesetz gerechtfertigt ist [29]. Das nDSG sieht diese Rechtfertigungsgründe ausdrücklich vor und konkretisiert diese [30]. Die Frage nach einer *Rechtfertigung* bedingt die Abwägung zwischen den Datenschutzinteressen der betroffenen Person und der Datenbearbeitung [31].

Da das nDSG nur personenbezogene Daten schützt [32], also Daten, die einen Rückschluss auf eine natürliche Person zu-

lassen, kann der Bearbeiter oder die Bearbeiterin seinen oder ihren Pflichten nachkommen, indem er oder sie die Daten anonymisiert. Dies hat den Vorteil, dass er oder sie die Daten statistisch weiterhin verwenden kann. Unter *Anonymisierung* ist das irreversible Entfernen oder Verändern von Personendaten zu verstehen, sodass jeder Bezug zur betroffenen Person ausgeschlossen ist [33]. Anonymisieren und Vernichten werden im nDSG in ihrer Funktion als gleichwertig beurteilt, wobei vorzugsweise eine Vernichtung der Daten vorgenommen werden sollte [34]. Die Formulierung «vernichten» nach Art. 6 Abs. 4 nDSG bedeutet die datenschutzkonforme Löschung der Daten. Der Datenträger muss nicht zerstört werden.

## 5. GESETZLICHE AUFBEWAHRUNGSPFLICHTEN ALS RECHTFERTIGUNGSGRUND

Zu den gesetzlichen Rechtfertigungsgründen nach Art. 31 Abs. 1 nDSG gehören Bearbeitungs-, Abklärungs- oder Aufbewahrungspflichten [35]. Letztere können sich aus unterschiedlichen Gesetzen ergeben.

**5.1 Aufbewahrungspflicht nach Rechnungslegungsrecht.** Art. 957 OR sieht eine Pflicht zur Buchführung und Rechnungslegung für Einzelunternehmen und Personengesellschaften, die einen Umsatzerlös von mindestens CHF 500 000 im letzten Geschäftsjahr erzielt haben, und für alle juristischen Personen. Demnach sind auch Stiftungen und Vereine buchführungspflichtig [36]. Die Rechnungslegung erfolgt im *Geschäftsbericht*. Dieser enthält mindestens die Jahresrechnung, die sich aus der Bilanz, der Erfolgsrechnung und dem Anhang zusammensetzt. Welche Rechenwerke und weiteren Angaben im Geschäftsbericht enthalten sein müssen, bestimmt sich nach der wirtschaftlichen Grösse eines Unternehmens [37].

Unter *Buchungsbeleg* wird das Schriftstück verstanden, aus dem sich die für eine einzelne Buchung relevanten Elemente ableiten lassen [38]. Insbesondere in diesen können personenbezogene Daten enthalten sein, die unter das DSG und nDSG fallen. Entsprechend stellt sich die Frage, ob einem an sich berechtigten Löschungsantrag nachgekommen werden muss, wenn die entsprechenden Personendaten sich in den Geschäftsbüchern und Belegen finden.

Die Geschäftsbücher und die Buchungsbelege sowie der Geschäftsbericht und der Revisionsbericht sind *während zehn Jahren* aufzubewahren [39].

Beantragt die betroffene Person die Löschung, widerspricht sie ausdrücklich der Datenbearbeitung. Diese ist damit grundsätzlich widerrechtlich. Da bereits das Aufbewahren und Speichern als Bearbeiten im Sinne des DSG und nDSG verstanden wird [40], ist auch die Aufbewahrung bzw. Speicherung der Personendaten in den Büchern und Buchungsbelegen widerrechtlich. Kommt der Datenbearbeiter oder die Datenbearbeiterin den gesetzlichen Aufbewahrungspflichten nach Art. 958*f* OR nach, so erfüllt er oder sie eine gesetzliche Pflicht im Sinne von Art. 31 nDSG. Damit kann ein Rechtfertigungsgrund für die Datenbearbeitung vorliegen. Denn es ist allgemein anerkannt, dass die gesetzliche Aufbewahrungspflicht nach Art. 958*f* OR einen datenschutzrechtlichen Rechtfertigungsgrund darstellt [41].

Datenbearbeiter und Datenbearbeiterinnen können somit die *Löschung verweigern,* wenn er oder sie die fraglichen Personaldaten im Rahmen des Rechnungslegungs- und Buchführungsrechts bearbeitet und die Dokumente gestützt auf die gesetzliche Pflicht während zehn Jahren aufbewahren muss. Eine darüberhinausgehende Bearbeitung darf jedoch nicht erfolgen, sofern vom Gesetz nicht vorgesehen. Gegebenenfalls greift ein anderer Rechtfertigungsgrund.

**5.2 Steuerrechtliche Aufbewahrungspflichten.** Auch das Steuerrecht sieht eine gesetzliche Aufbewahrungspflicht vor. Natürliche Personen mit Einkommen aus selbstständiger Erwerbstätigkeit und juristische Personen müssen Geschäftsbücher und sonstige Belege, die mit ihrer Tätigkeit in Zusammenhang stehen, ebenfalls während *zehn Jahren* aufbewahren [42].

Damit kann eine Datenbearbeitung gegen den ausdrücklichen Willen der betroffenen Person auch aus steuerrechtlichen Aufbewahrungspflichten gerechtfertigt sein. Das DBG bezweckt einen Gleichlauf zum Rechnungslegungs- und Buchführungsrecht. Eine über die Aufbewahrung bzw. Speicherung hinausgehende Datenbearbeitung ist jedoch nicht zulässig, sofern vom Gesetz nicht vorgeschrieben. Es ist aber nicht ausgeschlossen, dass ein anderer Rechtfertigungsgrund greift.

**5.3 MWST-rechtliche Aufbewahrungspflicht.** Bei der MWST richtet sich die Aufbewahrungsfrist nach Art. 70 Abs. 2 MWSTG. Demnach hat die steuerpflichtige Person ihre Geschäftsbücher, Belege, Geschäftspapiere und sonstigen Aufzeichnungen bis zum Eintritt der absoluten Verjährung der Steuerforderung ordnungsgemäss aufzubewahren [43]. Art. 958*f* OR bleibt dabei ausdrücklich vorbehalten.

Die absolute Verjährung der Steuerforderung tritt in jedem Fall *zehn Jahre* nach Ablauf der Steuerperiode ein, in der die Steuerforderung entstanden ist [44]. So lange sind die Geschäftsbücher, Belege, Geschäftspapiere und sonstigen Aufzeichnungen aufzubewahren.

Auch die MWST-rechtliche Aufbewahrungspflicht stellt einen Rechtfertigungsgrund nach Art. 31 Abs. 1 nDSG dar. Gestützt auf diesen kann der Datenbearbeiter oder die Datenbearbeiterin also ggfs. die Löschung rechtmässig verweigern und die Datenbearbeitung (Aufbewahrung und Speichern) fortsetzen. Eine darüberhinausgehende Datenbearbeitung ist jedoch nicht zulässig, sofern gesetzlich nicht vorgesehen. Eventuell greifen aber andere Rechtfertigungsgründe.

## 6. ÜBERWIEGENDES PRIVATES INTERESSE ALS RECHTFERTIGUNGSGRUND

Neben den gesetzlichen Aufbewahrungspflichten können auch überwiegende private Interessen eine Datenbearbeitung rechtfertigen, die entgegen einem berechtigten Löschungsanspruch erfolgt (Art. 31 nDSG).

Primär kommen die *Eigeninteressen* des Verletzenden, des Datenbearbeiters oder der Datenbearbeiterin in Betracht. Gegebenenfalls können auch überwiegende *Drittinteressen* eine Datenbearbeitung rechtfertigen [45]. Das nDSG listet nicht abschliessend auf, welche Interessen rechtfertigend wirken

können. In jedem Fall hat eine Interessensabwägung stattzufinden. Es bedarf also stets einer Einzelfallbetrachtung.

Neben den im nDSG gelisteten Interessen, die nachfolgend nicht weiter vertieft werden sollen, kann der Schutz von Eigentum und Rechten, insbesondere die *Durchsetzung oder Abwehr von Forderungen* ein berechtigtes privates Interesse darstellen [46].

Das nDSG äussert sich jedoch nicht dazu, wie lange Daten, die gegen den Willen des oder der Betroffenen und gestützt auf ein (überwiegendes) privates Interesse bearbeitet werden, aufbewahrt werden dürfen bzw. müssen. Dies ist abhängig davon, worauf das private Interesse gründet.

Für die datenschutzrechtliche Betrachtung der maximal zulässigen Aufbewahrungsdauer von personenbezogenen Daten (in Geschäftsunterlagen), die zur Durchsetzung oder Abwehr von Forderungen benötigt werden, ist die Verjährung dieser Forderungen ausschlaggebend [47].

*Verjährung* ist die Entkräftung einer Forderung durch Zeitablauf. Dabei kann die Forderung vertraglich oder ausservertraglich begründet sein. Diese Dichotomie ist prägend für das Schweizer Privatrecht und zeigt sich insbesondere im Verjährungsrecht. Für das anwendbare Verjährungsregime ist somit bei jeder Forderung zunächst der Anspruchstyp zu identifizieren [48].

*Vertragliche Ansprüche* verjähren regelmässig nach zehn Jahren. Dieser Grundsatz wird durch zahlreiche Ausnahmen im OR oder durch Nebengesetze durchbrochen, die kürzere Fristen vorsehen [49].

Ausservertragliche Ansprüche beruhen auf Deliktsrecht (Art. 41 ff. OR) oder Bereicherungsrecht (Art. 61 ff. OR). Für diese Ansprüche gilt eine doppelte Verjährungsfrist: die relative und die absolute Verjährungsfrist. Für die Frage der zulässigen Aufbewahrungsdauer von Personendaten ist auf die *absolute Verjährungsfrist* abzustellen.

Die für die Frage nach der datenschutzrechtlichen Rechtfertigung nicht weiter relevante relative Verjährungsfrist von Ansprüchen aus *Delikten* verjähren nach drei Jahren. Die absolute Verjährungsfrist beträgt *zehn Jahre,* vom Tage an gerechnet, an dem das schädigende Verhalten erfolgte oder aufhörte. Bei Tötung eines Menschen oder bei Körperverletzung verjährt der Anspruch auf Schadenersatz oder Genugtuung absolut nach *20 Jahren* [50].

Neben Vertrag und unerlaubter Handlung (Delikt) regelt das OR in Art. 62 ff. als dritten Entstehungsgrund für Forderungen die *ungerechtfertigte Bereicherung*. Der Bereicherungsanspruch verjährt mit Ablauf von drei Jahren, nachdem der Verletzte von seinem Anspruch Kenntnis erhalten hat, in jedem Fall aber mit Ablauf von *zehn Jahren* seit der Entstehung des Anspruchs (absolute Verjährungsfrist, vgl. Art. 67 Abs. OR).

Neben der Frage der relevanten Verjährungsfrist als Aufbewahrungsfrist ist für die Interessensabwägung die Frage nach

der *Wahrscheinlichkeit,* dass Forderungen geltend gemacht oder abgewehrt werden müssen, ausschlaggebend. Besteht kein Risiko, kann wohl kaum ein überwiegendes Interesse an der Datenbearbeitung begründet werden. Besteht hingegen ein Risiko, ist eine Abwägung zwischen den Interessen des Datenbearbeiters oder der Datenbearbeiterin und der betroffenen Person vorzunehmen. Anschliessend muss geprüft werden, ob die vom Löschungsanspruch betroffenen Daten für die Geltendmachung oder Abwehr von Forderungen überhaupt nötig sind. Trifft dies zu, so dürfen diese Daten aufbewahrt und gespeichert und ggfs. in einem allfälligen Streitfall verwendet werden. In diesem Fall kann ein Rechtfertigungsgrund nach Art. 31 nDSG vorliegen. Die Daten dürfen dann so lange bearbeitet werden, wie die (absolute) Verjährung noch nicht eingetreten ist. Denn so lange kann sich der Datenbearbeiter oder die Datenbearbeiterin mit allfälligen Ansprüchen konfrontiert sehen oder selbst Forderungen geltend machen. Nach Eintritt der (absoluten) Verjährung sind die vom Löschungsantrag umfassten Daten allesamt zu löschen.

Es ist denkbar, dass mehrere Rechtfertigungsgründe erfüllt sind und damit auch unterschiedliche Aufbewahrungsfristen zu beachten sind. Bei einer solchen Kollision ist zu prüfen, ob alle vom Löschungsanspruch umfassten Daten für den jeweiligen Rechtfertigungsgrund relevant sind. Ist dies der Fall, ist auf die längste Frist abzustellen. Ist dies nicht der Fall, müssen für die jeweiligen Daten die unterschiedlichen Aufbewahrungsfristen berechnet werden.

## 7. ZUSAMMENFASSENDE BETRACHTUNG

Die Datenbearbeitung nach dem nDSG hat nach den gleichen Grundsätzen zu erfolgen wie bis anhin. Dies bedeutet, dass eine Datenbearbeitung, die diesen Grundsätzen folgt, zulässig ist. Damit benötigt der Datenbearbeiter oder die Datenbearbeiterin nicht stets einen Rechtfertigungsgrund für die Datenbearbeitung (wie dies in der EU der Fall ist).

Verlangt die betroffene Person hingegen, die sie betreffenden Daten zu löschen, so ist dem grundsätzlich nachzukommen. Denn eine Datenbearbeitung gegen den Willen der betroffenen Person ist widerrechtlich und stellt eine Persönlichkeitsverletzung dar. Allerdings kann es vorkommen, dass eine widerrechtliche Datenbearbeitung gerechtfertigt werden kann. Namentlich kann die Erfüllung einer gesetzlichen Pflicht eine Datenbearbeitung, die gegen den Willen der betroffenen Person erfolgt, rechtfertigen. Auch ein überwiegendes privates Interesse kann einen Rechtfertigungsgrund darstellen. Ob dies in der fraglichen Konstellation der Fall ist, muss jeweils gesondert geprüft werden.

Liegt ein Rechtfertigungsgrund vor, stellt sich die Frage, wie lange die Datenbearbeitung (noch) erfolgen darf. Eine unbefristete Datenbearbeitung würde das Recht der betroffenen Person auf informationelle Selbstbestimmung unverhältnismässig einschränken. Daher sind die gesetzlichen oder sich aus dem Verjährungsrecht ergebenden Aufbewahrungsfristen zu beachten. Diese können für die Dauer der Aufbewahrung einem an sich berechtigten Löschungsanspruch entgegenstehen und die Datenbearbeitung rechtfertigen.

Trotz der Stärkung der Betroffenenrechte im nDSG gilt der Löschungsanspruch nicht absolut. Der Datenbearbeiter oder die Datenbearbeiterin tut also gut daran, nach Erhalt eines solchen Antrags genau zu prüfen, ob dem Löschungsanspruch nachgekommen werden muss. ■

**Fussnoten: 1)** Verordnung 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO). **2)** Art. 4 Abs. 1 bis 3 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG). **3)** Art. 4 Abs. 4 und Abs. 5 DSG. **4)** Art. 5 DSG. **5)** BBl 2017 6941, S. 6982. 6) Baeriswyl, in Baeriswyl/Pärli (Hrsg.), Datenschutzgesetz (DSG), Art. 4 N. 1; David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020. **7)** Siehe die praktisch identischen Formulierungen der Grundsätze in Art. 6 nDSG. **8)** Gemäss Art. 6 Abs. 1 DSGVO sind Rechtfertigungsgründe: Einwilligung, Vertragserfüllung, rechtliche Verpflichtungen, überwiegende persönliche oder öffentliche Interessen. **9)** Reimer, in Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Nomos Kommentar, Art. 6 N. 1. **10)** BBl 2017 6941, S. 6972. **11)** BBl 2017 6941, S. 6973 f.; vgl. Art. 60 ff. nDSG. **12)** Als Auftragsbearbeiter werden Dritte (Firmen oder Personen) bezeichnet, denen qua Vertrag oder Gesetz die Datenbearbeitung übertragen wird. Gemäss dem nDSG ist das Outsourcen von Datenbearbeitungen nach wie vor zulässig, sofern die Daten so bearbeitet werden, wie der oder die Verantwortliche selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet, vgl. Art. 9 Abs. 1 nDSG. **13)** Art. 12 Abs. 5 nDSG; vgl. auch die Konkretisierung in Art. 26 des Vorentwurfs zur Verordnung zum nDSG, wonach Unternehmen und andere privatrechtliche Organisationen, die am Anfang eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt: Es werden umfangreich besonders schützenswerte Personendaten bearbeitet oder es wird ein Profiling mit hohem Risiko durchgeführt. **14)** Art. 22 nDSG. **15)** Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte/-r, dem/der im nDSG ein ganzes Kapitel gewidmet ist. **16)** Art. 24 nDSG. **17)** Art. 33 Abs. 1 DSGVO. **18)** Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 92. **19)** Art. 14 Abs. 1 DSG. **20)** Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 99. **21)** Bundesamt für Justiz, Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, S. 30/87. **22)** Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 100. **23)** Art. 13 Abs. 2 Bundesverfassung (BV); Rudin, in Baeriswyl/Pärli (Hrsg.), Datenschutzgesetz (DSG), Art. 8 N. 1. **24)** BGE 126 I 7, 12 E. 3.c. aa; BGE 138 I 256, 262 E. 5.5; OFK-Kommentar, Biaggini, Bundesverfassung, Art. 13 N. 14. 25) BBl 2017 6941, S. 7071. **26)** Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 38. **27)** Art. 30 Abs. 2 lit. b nDSG. **28)** Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 38. **29)** So auch Art. 28 Abs. 2 ZGB, vgl. auch BBl 2017 6941, S. 7073. **30)** Art. 31 nDSG. **31)** BBl 2017 6941, S. 7073; Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 41. **32)** Art. 2 Ab. 1 nDSG. **33)** Jöhri, Handkommentar DSG, Art. 21 N 28. **34)** BSK DSG-Bühler, Art. 21 N 22. **35)** BBl 201 6941, S. 7073. **36)** Vgl. Art. 69*a* und Art. 83*a* ZGB; ausgenommen hiervon sind Vereine und Stiftungen, die nicht verpflichtet sind, sich ins Handelsregister eintragen zu lassen, und Stiftungen, die nach Art. 83*b* Abs. 2 ZGB von der Pflicht zur Bezeichnung einer Revisionsstelle befreit sind. **37)** Vgl. zum Ganzen Müller/Henry/Barmettler, Rechnungslegung nach Obligationenrecht, veb.ch Praxiskommentar, Art. 958 N. 34 f. **38)** BSK OR II-Neuhaus/Suter, Art. 958*f* N. 9; hierzu zählen Bankbelege, Kassenbelege, Quittungen, Spesenbelege, Rechnungen und Zeiterfassungen von Mitarbeitenden. **39)** Art. 958*f* Abs. 1 OR; siehe auch die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV). **40)** Art. 4 lit. e DSG und Art. 5 lit. d nDSG. **41)** BSK DSG-Rampini, Art. 13 N. 18. **42)** Art. 126 Abs. 3 Bundesgesetz über die direkten Steuern (DBG), der auf Art. 957 ff. OR verweist. **43)** Geschäftsunterlagen, die im Zusammenhang mit der Berechnung der Einlageentsteuerung und des Eigenverbrauchs von unbeweglichen Gegenständen benötigt werden, sind während 20 Jahren aufzubewahren, vgl. Art. 70 Abs. 3 MWSTG. **44)** Art. 42 Abs. 6 MWSTG. **45)** Wermelinger, in Baeriswyl/Pärli (Hrsg.), Datenschutzgesetz (DSG), Art. 4 N. 1. **46)** BGE 136 II 508, E. 6.3.3. **47)** Kettler, Die Aufbewahrung von Geschäftsakten aus Sicht des Datenschutzes, datenschutzpraxis.ch, Factsheet Nr. 01 vom 24. Dezember 2019, S. 4. **48)** Moser, Haftung/Verjährungsfristen der vertraglichen und ausservertraglichen Haftung, in: Die Verjährung, HAVE, 2018, S. 20. **49)** Schwenzer/Fountoulakis, Obligationenrecht Allgemeiner Teil, Rz. 84.01 f. **50)** Art. 60 OR.